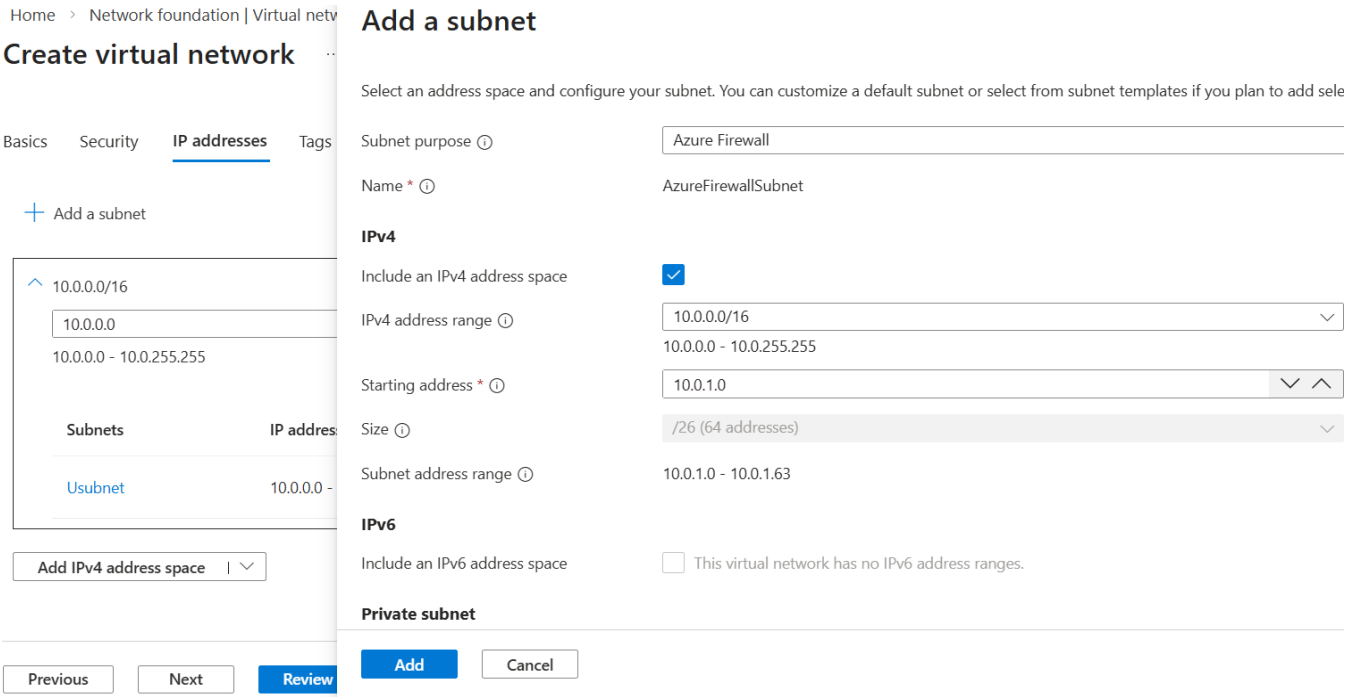
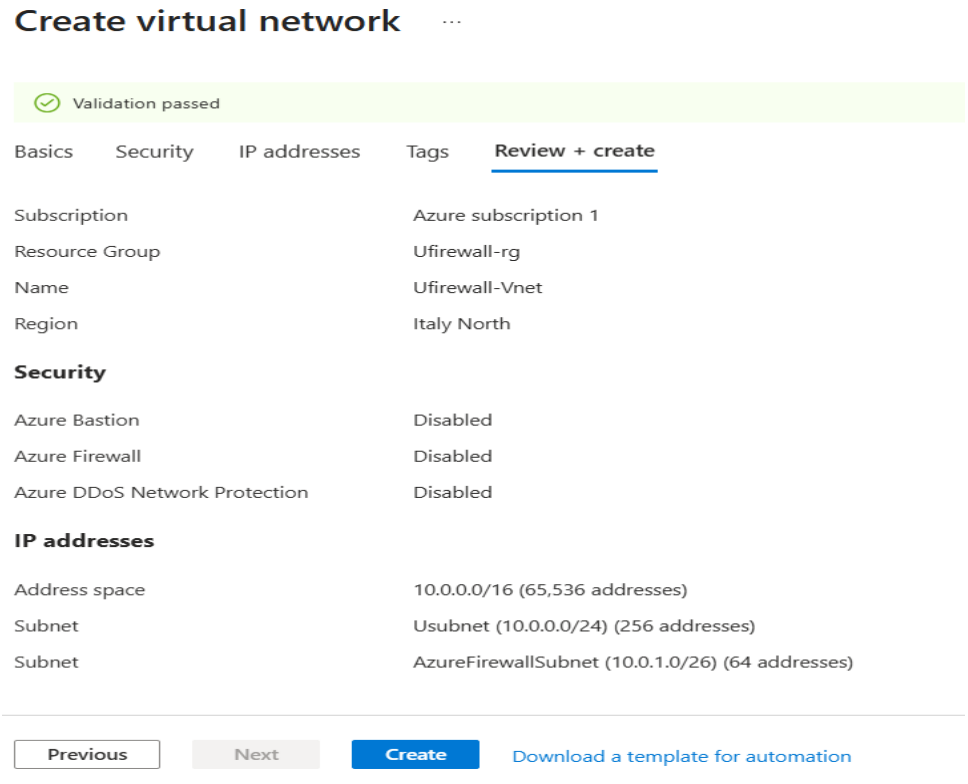
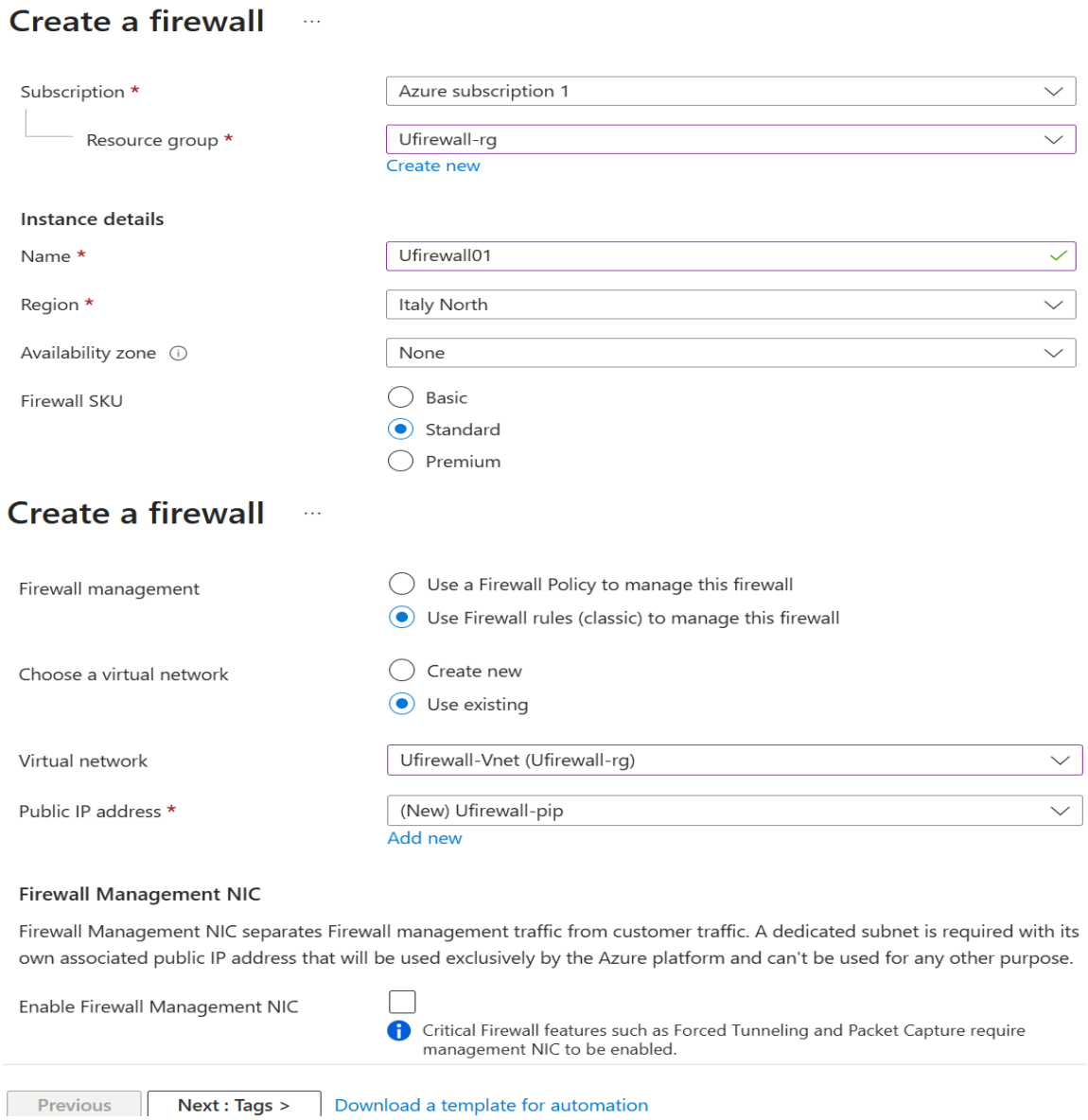
Azure Firewall

- ✓ **Create Rg-italy**
- ✓ **Create FirewallVnet with two subnets 1.default(subnet), 2. firewall (firewall subnet) Dedicated subnet**
- ✓ **Next Create SpokeVm with SpokeVnet and its subnet.**





✓ **Now lets Create Firewall**



✓

✓

✓

✓

✓

✓

✓

✓

✓ **Next create SpokeVm in same region and give its subnet.**

Create a virtual machine

Help me create a low cost VM

Validation passed

Help me create a low cost VM | Help me create a VM optimized for high avai

Subscription	Azure subscription 1
Resource group	(new) Uspoke-rg
Virtual machine name	Uspoke-vm
Region	Italy North
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Standard
Image	Windows Server 2025 Datacenter - Gen2
VM architecture	x64
Size	Standard D2ads v5 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	azureuser
Public inbound ports	RDP
Already have a Windows license?	No
Azure Spot	No

Networking

Virtual network	vnet-italynorth
Subnet	snet-italynorth-1
Public IP	(new) Uspoke-vm-ip
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled

Uspoke-vm

Virtual machine

Help me copy this VM in any region | Manage this VM with Azure CLI

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Connect
- Networking
- Settings
- Availability + scale
- Security

Uspoke-vm virtual machine agent status is not ready. Troubleshoot the issue →

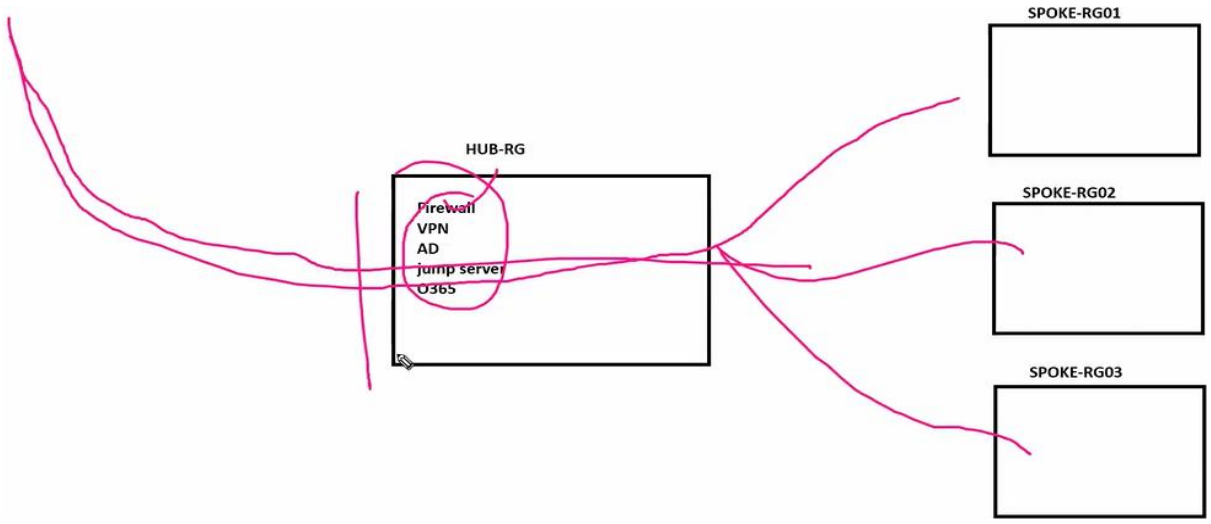
Help me copy this VM in any region

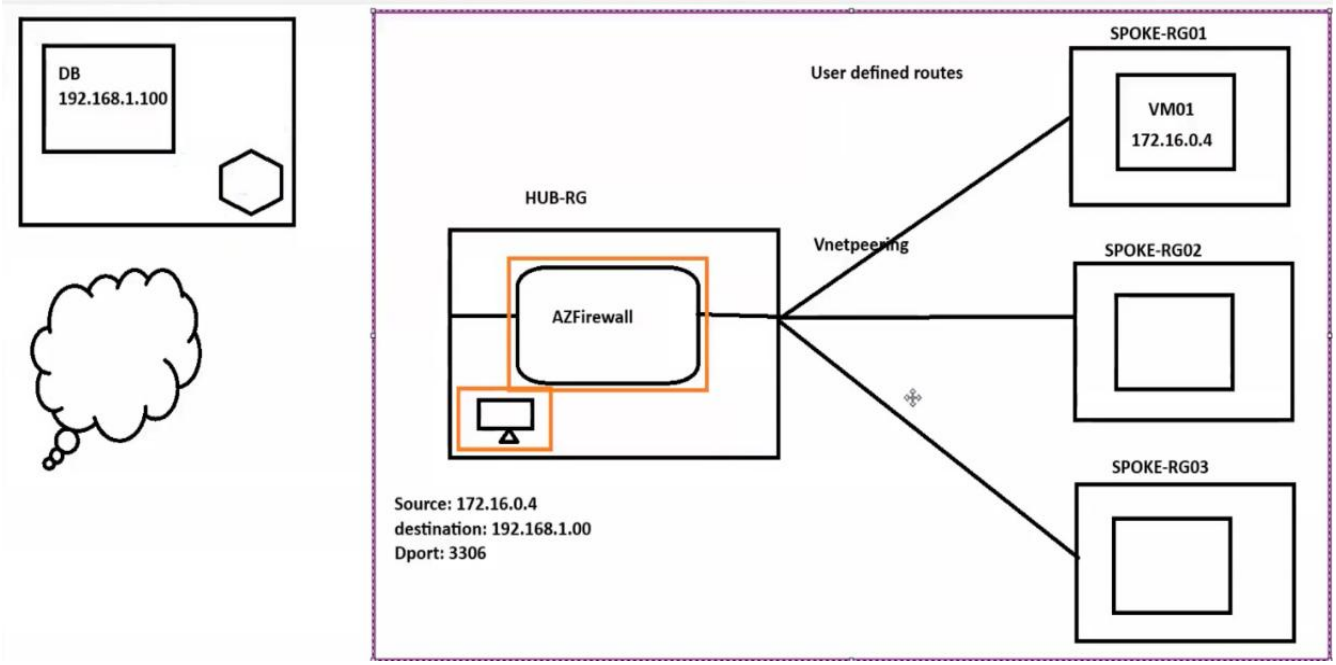
Connect | Start | Restart | Stop | Hibernate | Capture | Delete | Refresh | Scale | Open in mobile | Feedback

Essentials

Resource group (move)	: Uspoke-rg	Operating system	: Windows
Status	: Running	Size	: Standard D2ads v5 (2 vcpus, 8 GiB memory)
Location	: Italy North	Primary NIC public IP	: 172.213.227.14
Subscription (move)	: Azure subscription 1		1 associated public IPs
Subscription ID	: 5d75b66d-66bf-44e0-8d7e-7e61e4b043d7	Virtual network/subnet	: vnet-italynorth/snet-italynorth-1
		DNS name	: Not configured
		Health state	: -
		Time created	: 13/02/2026, 10:24 UTC

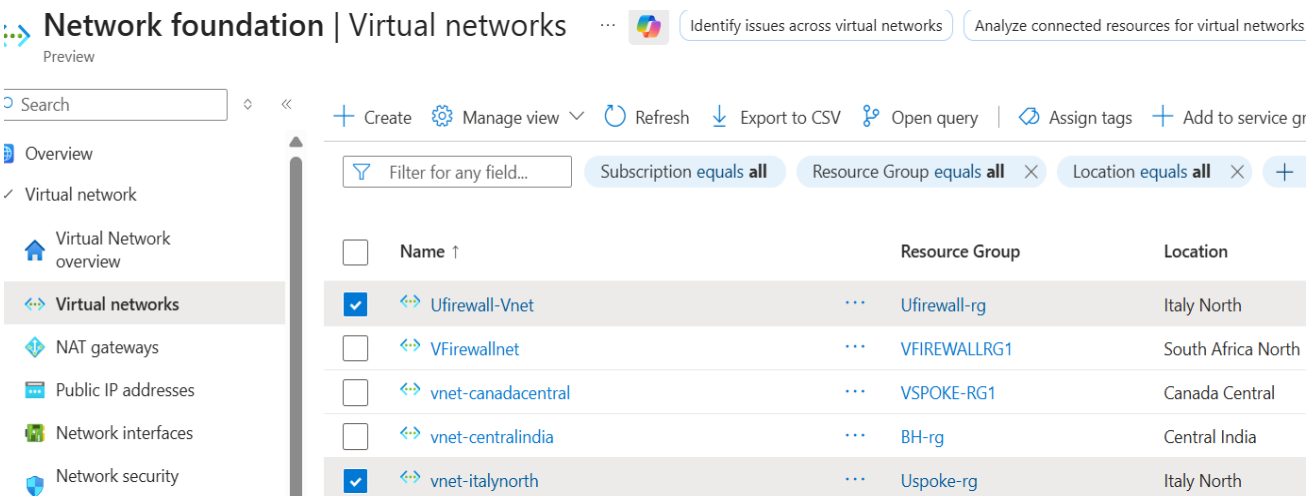
HUB & Spoke Architecture



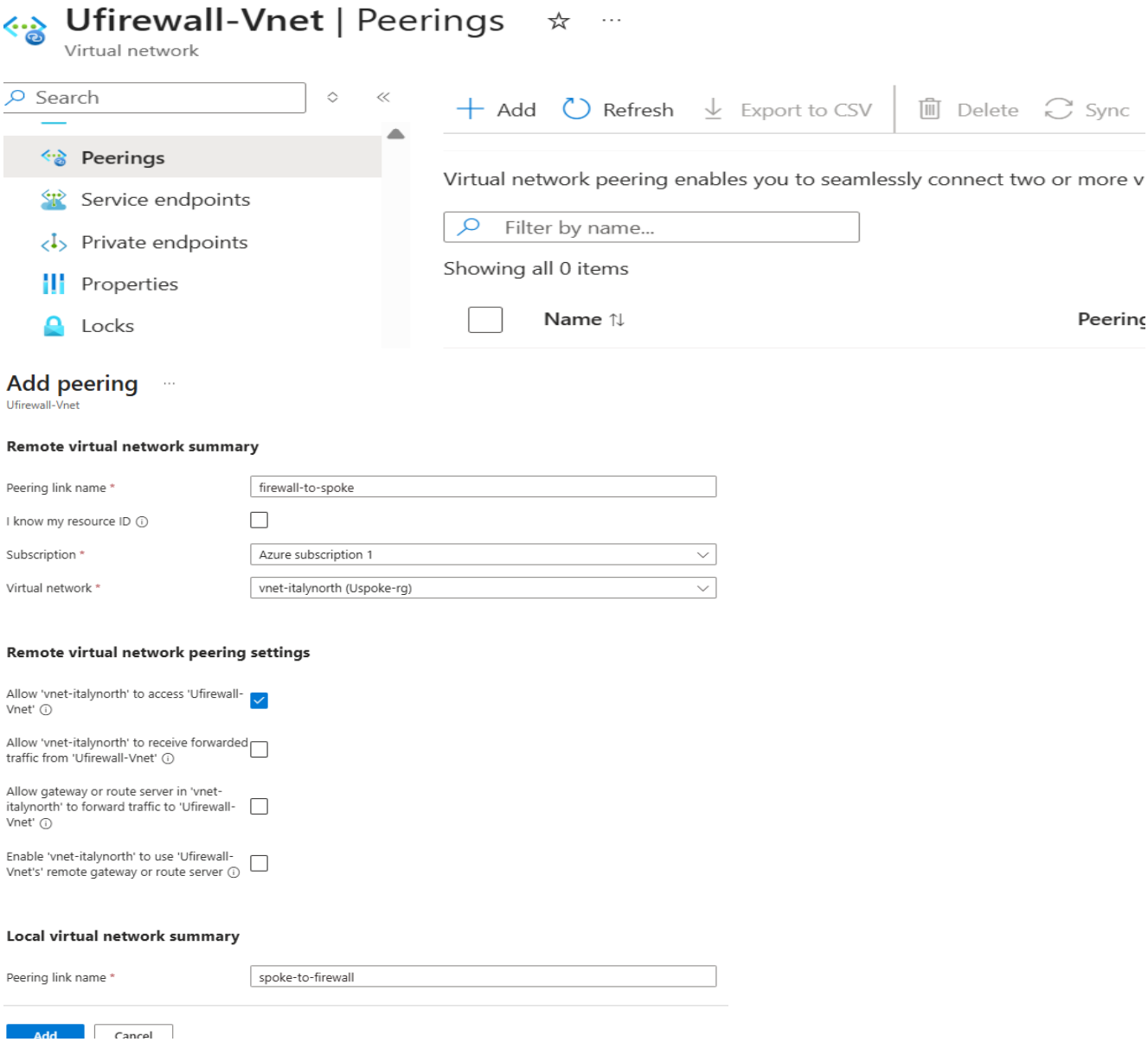


- ✓ **Machines behind the firewall, by default there will be denied rule we can't access the machines**
- ✓ **From public even though machines have public Ip once the machine is behind the firewall by default traffic will be blocked.**
- ✓ **For now, we created Firewall and Spokevm (windows)**
- ✓ **Let's log into spokevm(pip)**
- ✓ **Next Lets config Vnet peering from firewallVnet & SpokeVnet**

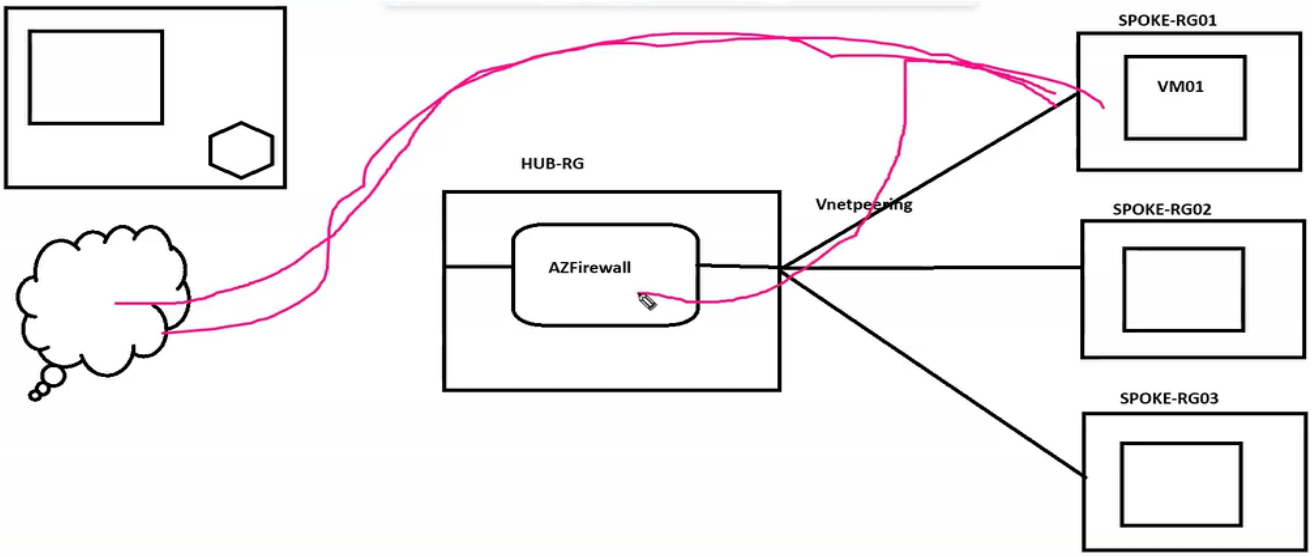
✓ **We see two diff Vnet for firewall and spoke below**



✓ **Choose any Vnet for peering**



- ✓ **After Vnet peering we can still connect to spokeVm bcz the traffic is going through outside and connecting to spokeVm.**



- ✓ **Let's Redirect traffic to firewall**
- ✓ **For that use should right Route Table (User Defined Routes)**
- ✓ **Search for Route Tables and click on Create**

Create Route Table ...

Basics Tags Review + create

Select the subscription to manage deployed resources and costs. Use resource groups like folde
manage all your resources.

Subscription * ⓘ — Azure subscription 1

Resource group * ⓘ — Uspoke-rg

Create new

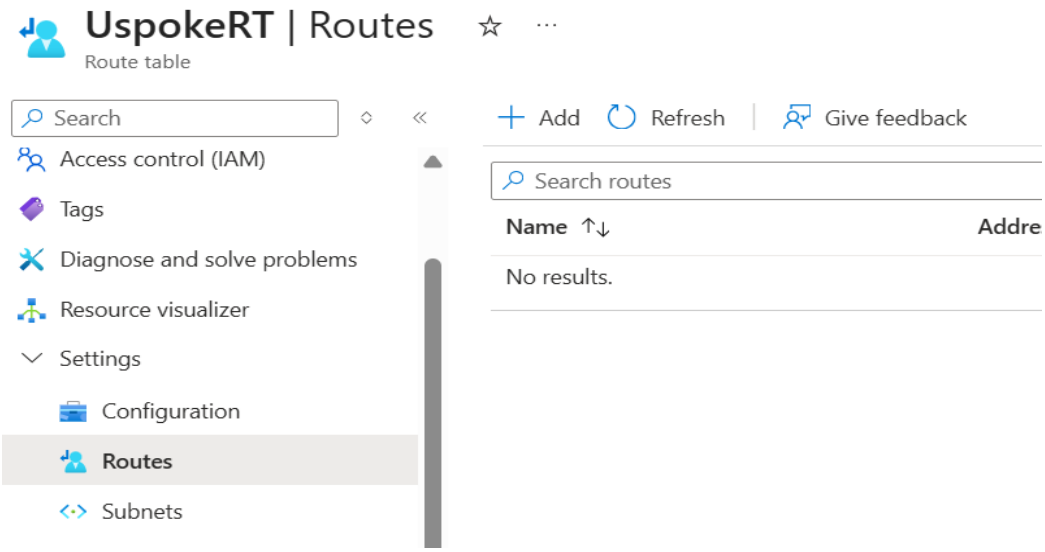
Instance details

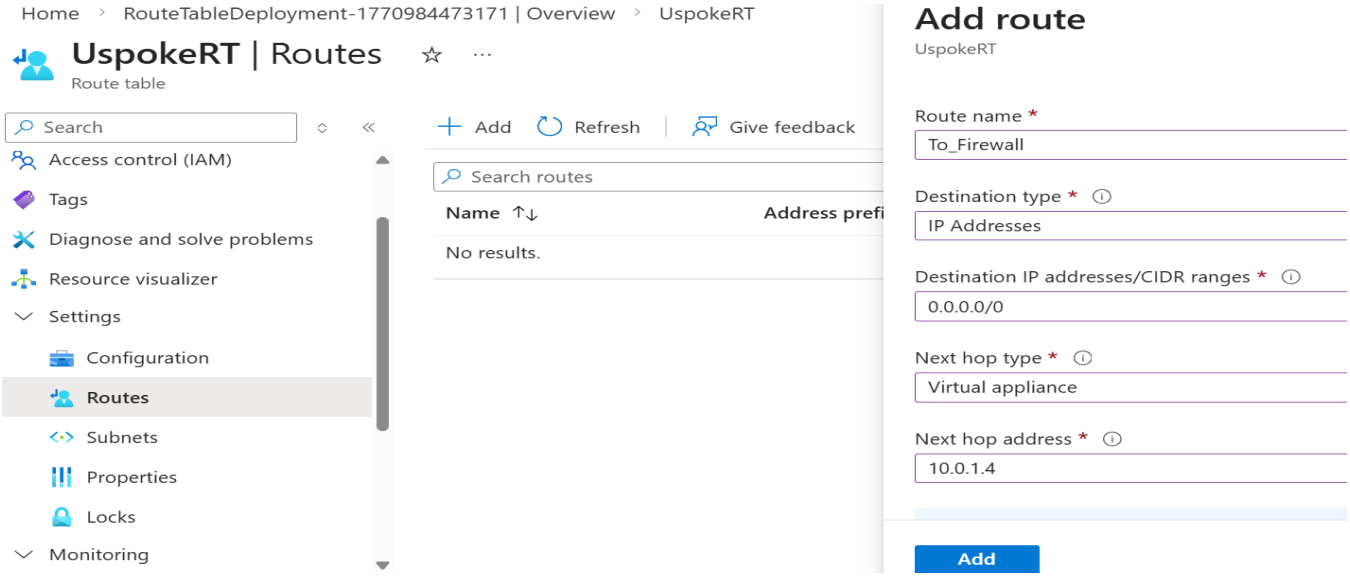
Name * ⓘ — UspokeRT

Propagate gateway routes * ⓘ — ◯ Yes ◯ No

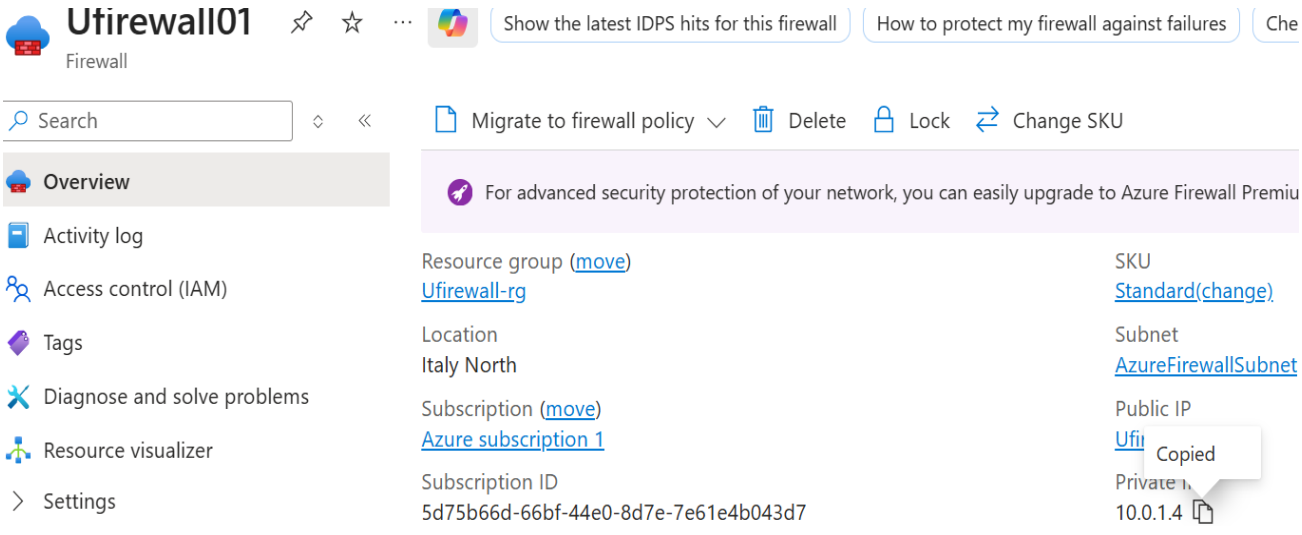
Region * ⓘ — (Europe) Italy North

✓ **Below click on Add and add route**

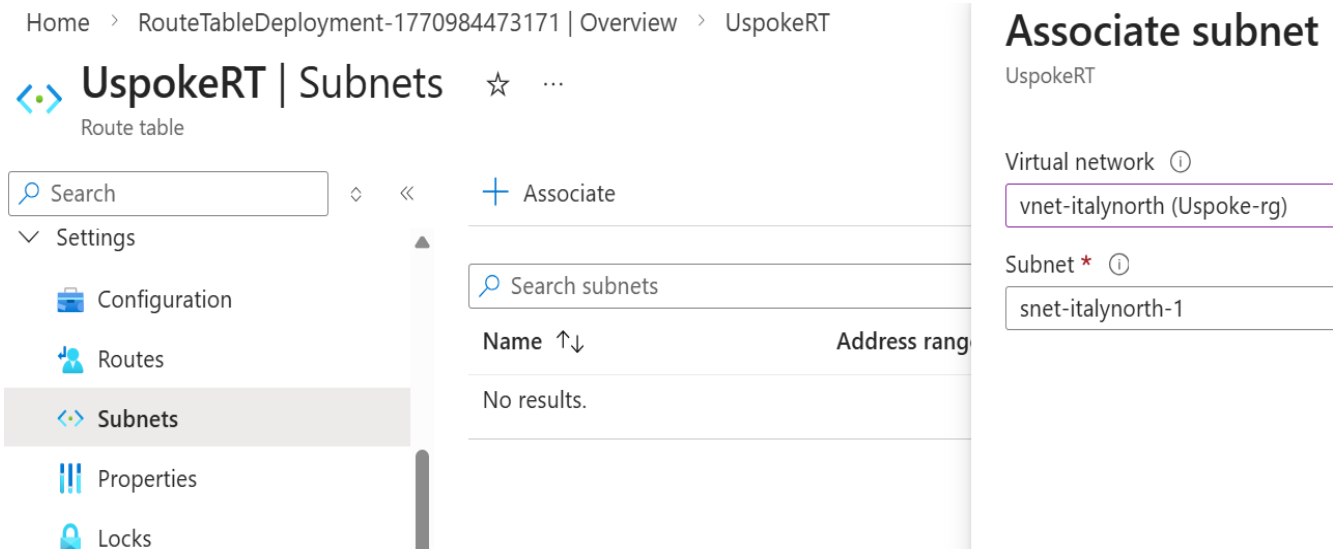




✓ **0.0.0.0/0 is Any above. Copy below Firewall Private Ip Below**

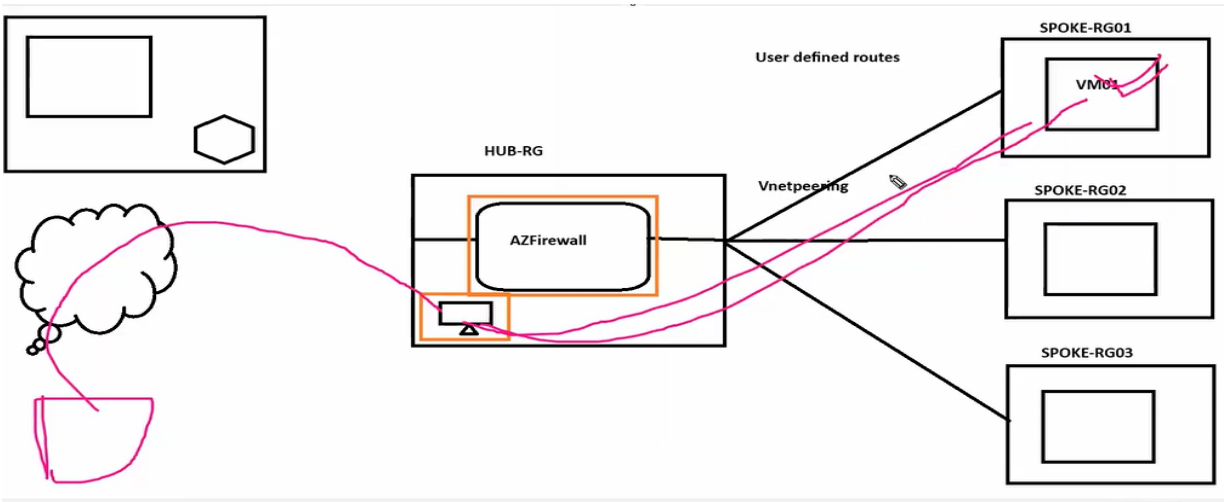


- ✓ **Now from SpokeVm whatever the traffic it should hit firewall first**
- ➢ **Now Next Once We Write the Route rule it should be attached to Subnet**

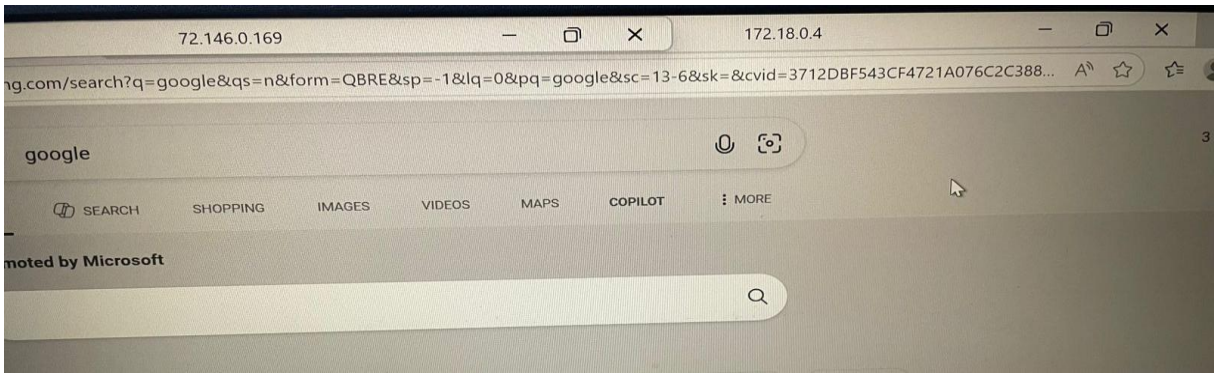


- ✓ **We have defined Routing, so the traffic coming from inside it should use Azure Firewall only, the traffic will flow from firewall only.**
- ✓ **After adding the rules to subnet automatically SpokeVM which is logged in earlier it will disconnect, Bcz traffic Diverted from firewall.**

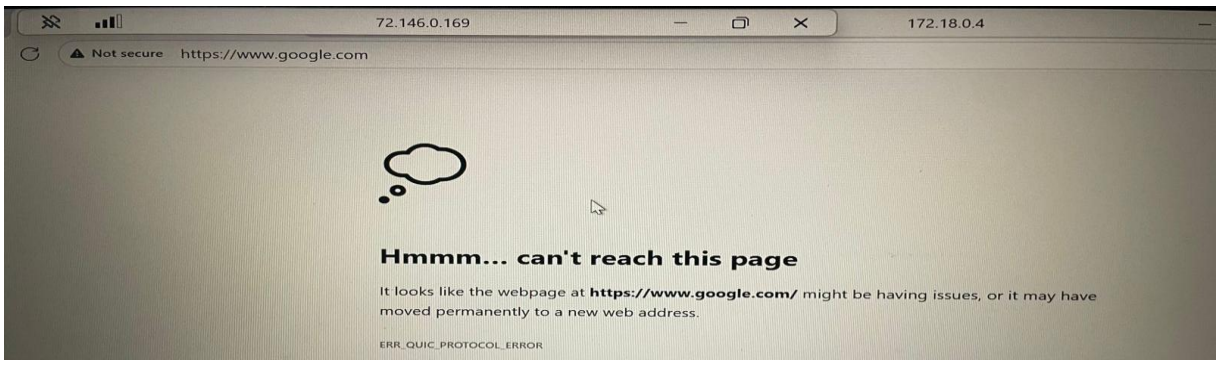
- Next create another VM using subnet in FirewallVnet.
- This VM just to know what's happening in SpokeVM.
- To access this from my LAPTOP→VM→SPOKEVM



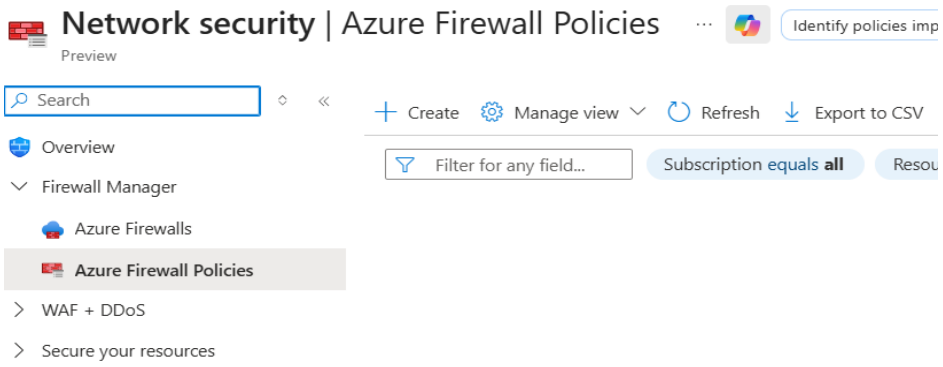
- ✓ Let's create VM (windows) on HUB-RG(FirewallVnet)
- ✓ Now Connect to this VM using PublicIP(72.146.0.169) on RDC
- ✓ After connecting to VM, open RDC in it and Connect to SpokeVM internally by using SpokeVM PrivateIP(172.18.0.4)

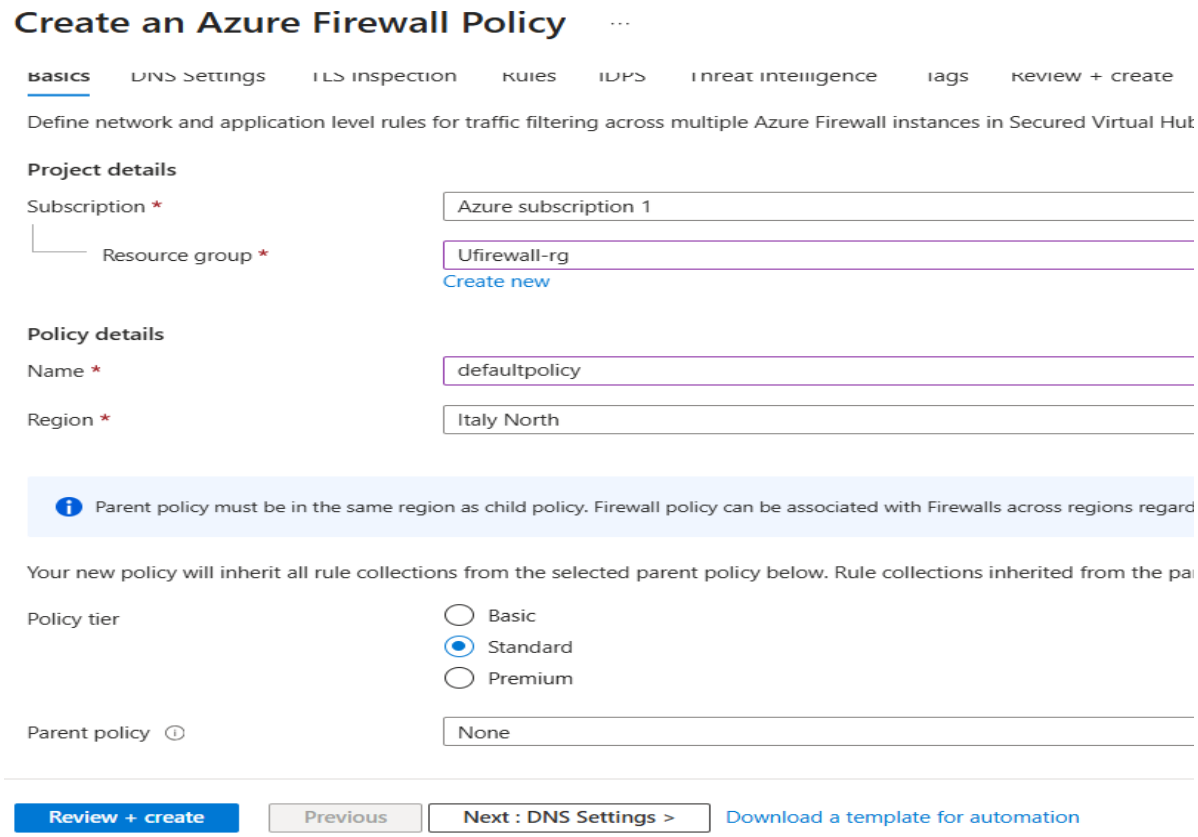


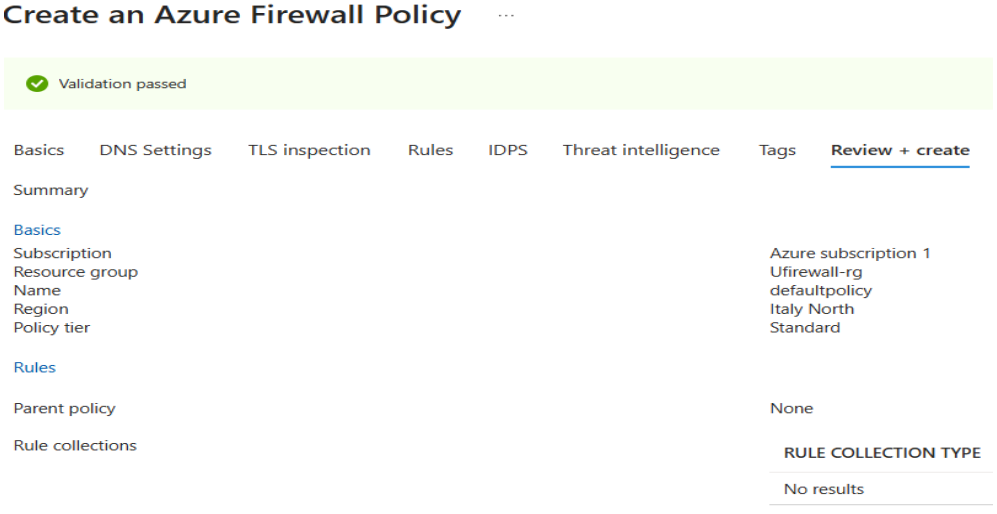
- ✓ We can't access anything bcz internet is not allowed and rules not match on firewall and this is behind the firewall.

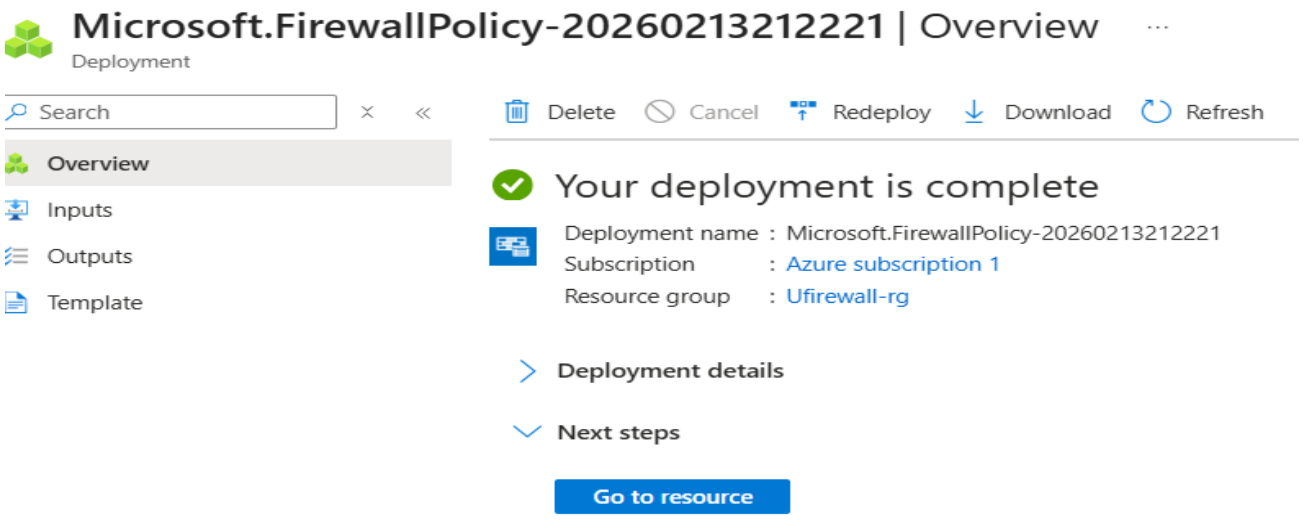


❖ Let's talk about Rules (follow below steps)

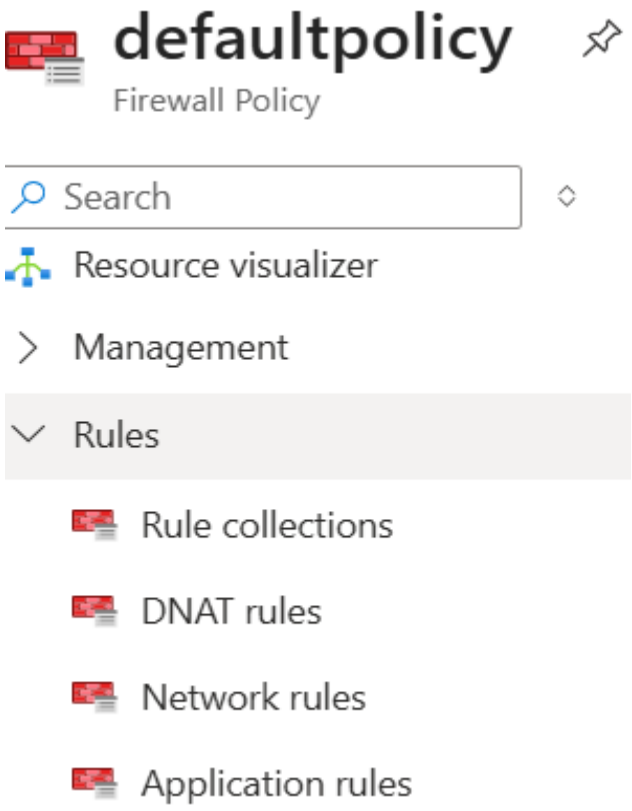






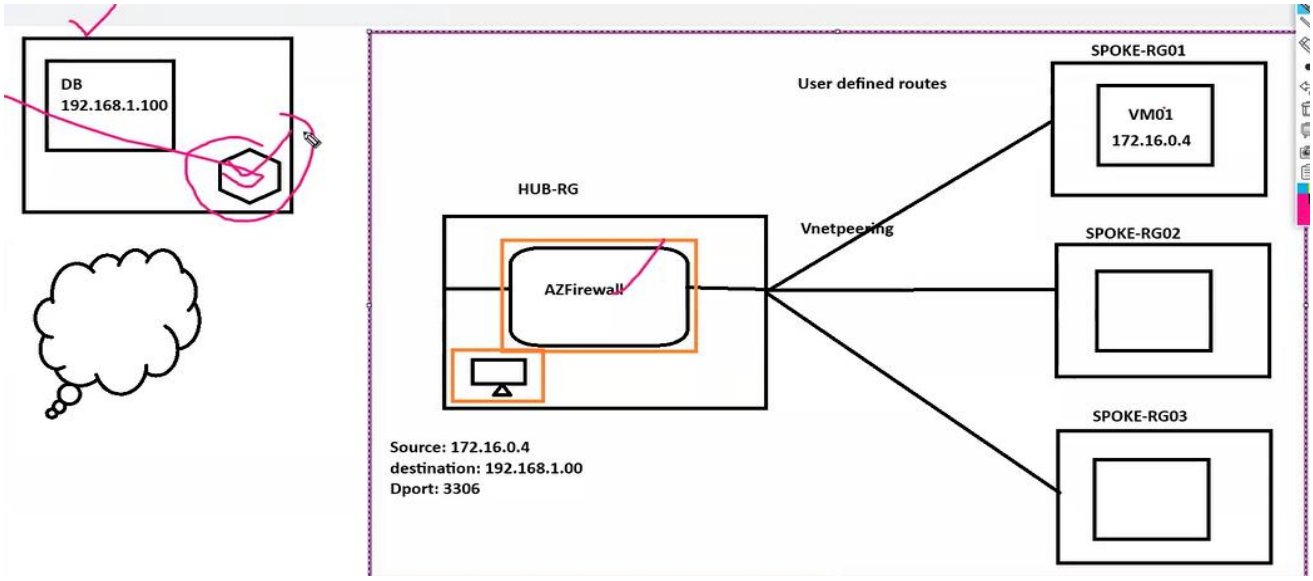


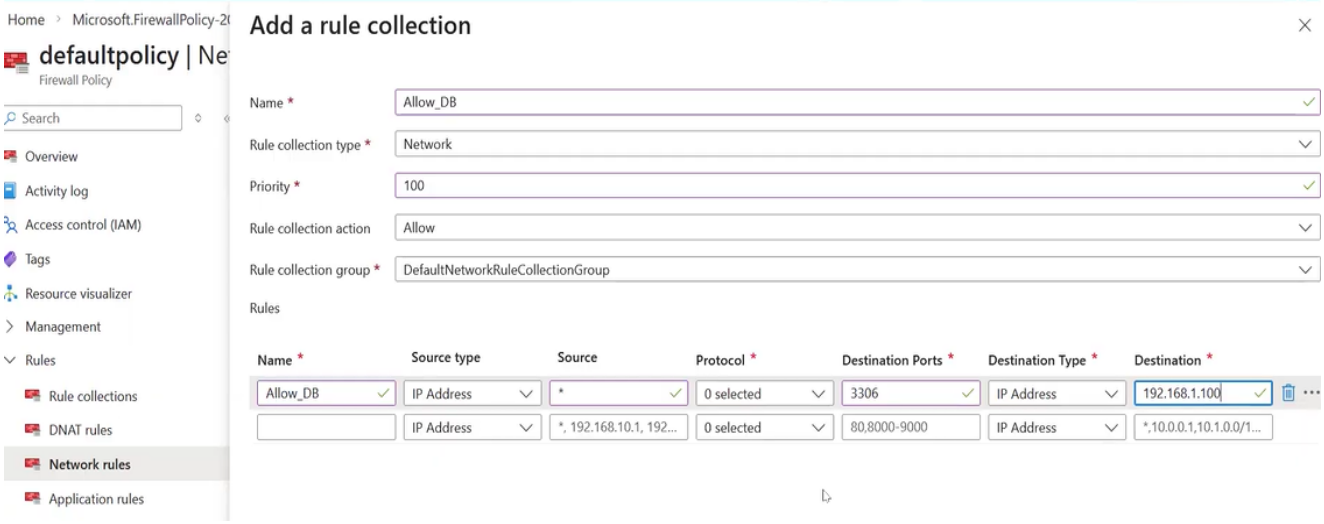
- ✓ **Created Name(defaultpolicy) but we didn't added rules in it, let's do that.**



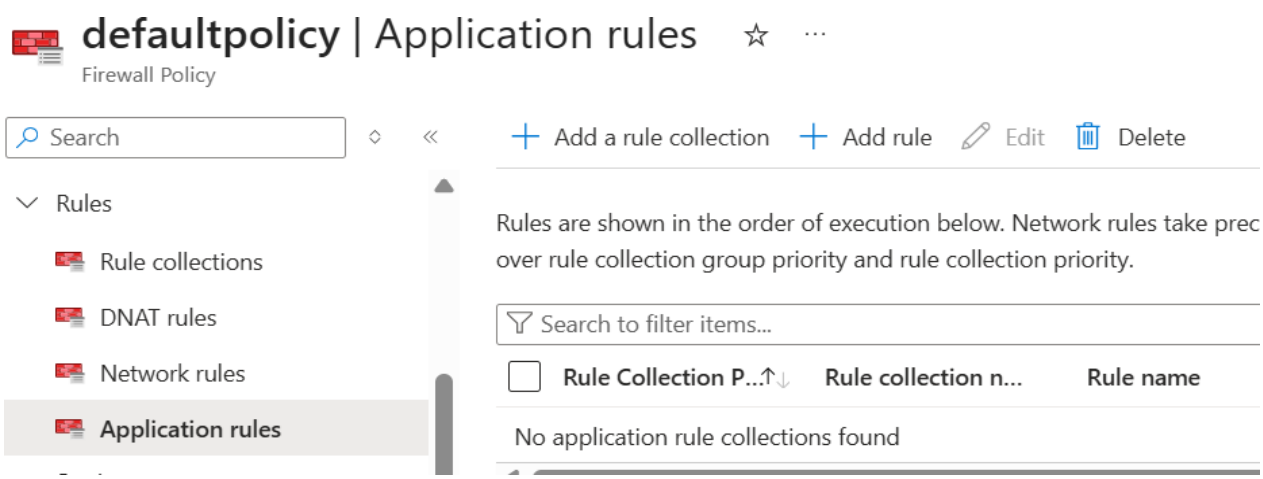
- ✓ **Network rule if we want to allow IP to IP then we use it.**
- ✓ **We don't use domain names here**
  - **Below you can see example which we used in lab.**

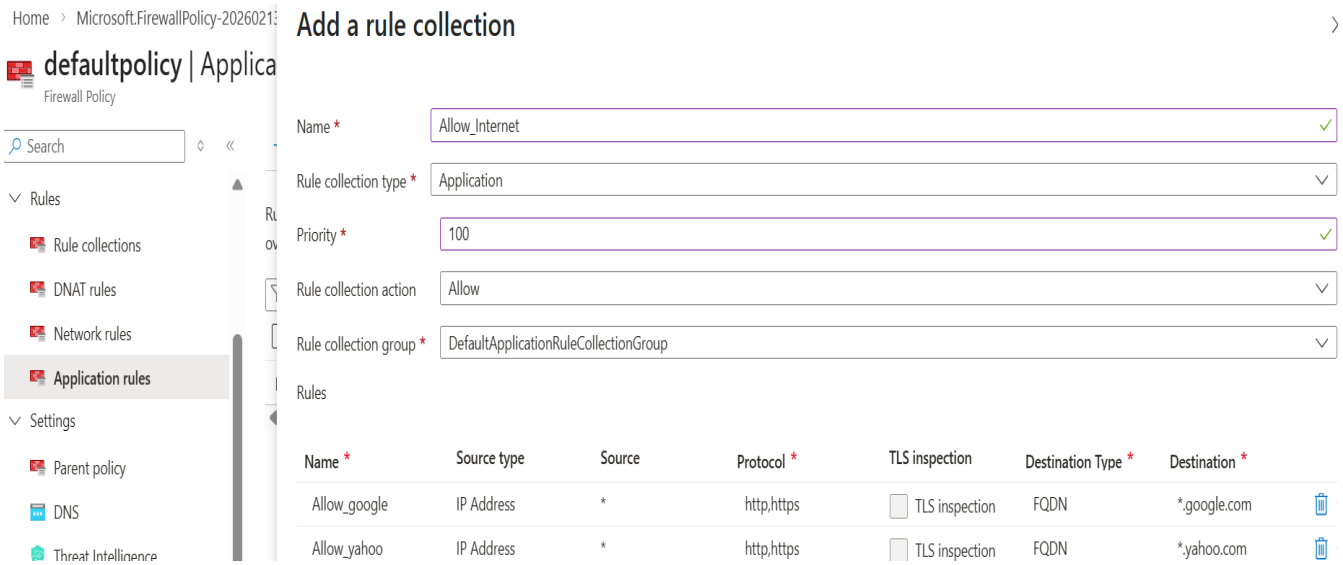
✓ **App & DB in different datacentres and they both have firewalls and both should config firewall rules then only we can access both.**





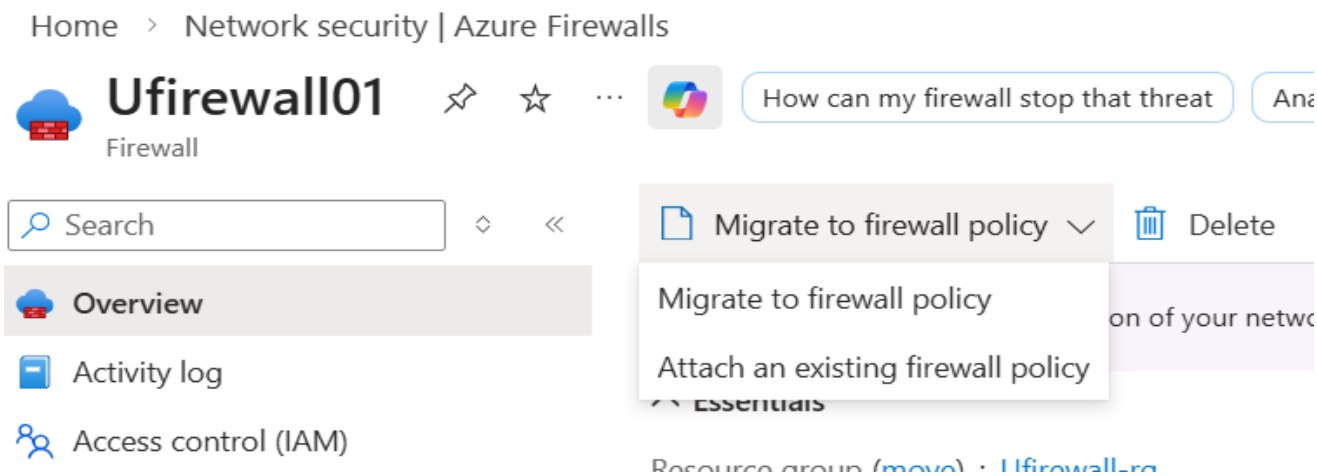
❖ **Application rules**

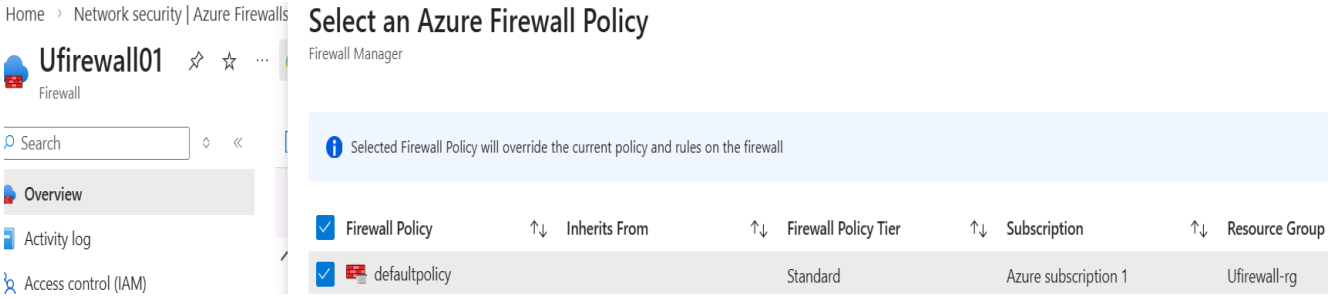




✓ **Associate this defaultpolicy to your Firewall**

✓ **Go to firewall→Migrate to firewall policy→Attach an existing firewall policy below**

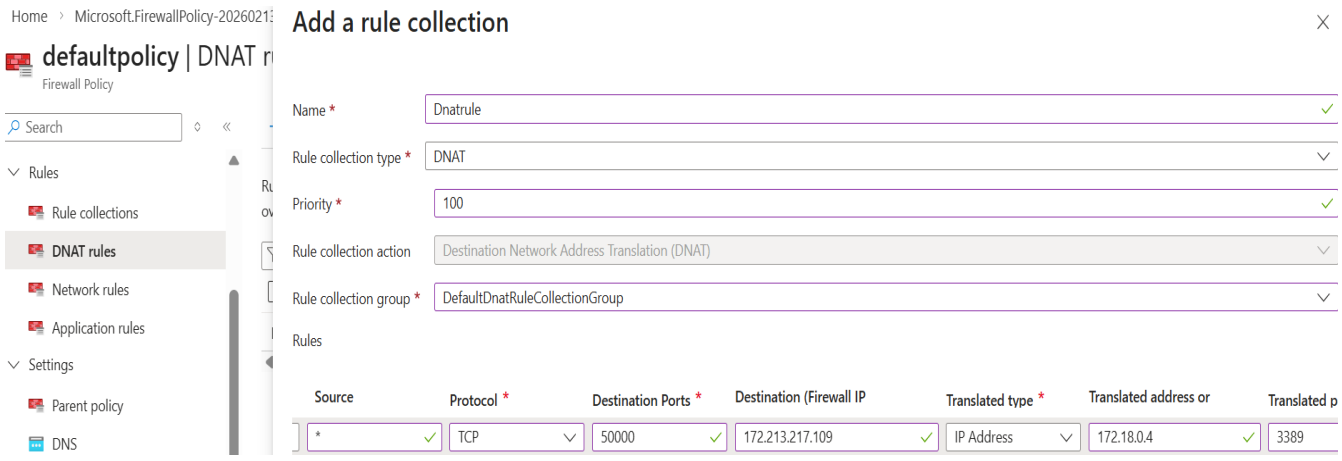




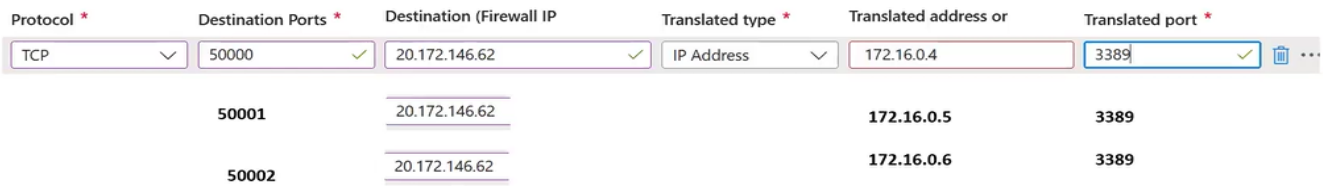
✓ **Select above policy and save.**

❖ DNAT rules

- ✓ Below I want to connect from internet to backend machine.
- ✓ Like from My laptop to directly Backend machine, but we can't connect bcz the machine is behind the firewall.
- ✓ But in this case, we can cannot by use Firewall Pubilc IP
- ✓ Outside traffic hits to Firewall Public IP from that traffic will go to Backend machine, here Backend Private IP masked by firewall.
- ✓ Firewall PublicIP (172.213.217.109)→Backend SpokeVM PrivateIP (172.18.0.4)
- ✓ Same with ports 50000→3389
- ✓ Translating with Public→Private and from Port→Port for Security to Machine, we are just Mapping with one to one.
- ✓ We can choose servers; on those we can add this Mapping at in emergency situations then access backend machines.



Example Below:



- There is another option DNATTING→we connect with Private IPs only by using VPS, we can login into the azure infrastructure to one of the gem servers from there we are going to connect.

✓ **Copy firewallPublicIP:50000**

✓ **By this we can connect to Backend SpokeVM**